20. *Mikheev V.A.* Osnovy postroeniya podsistemy zashchity informatsii mnogofunktsional'noy informatsionnoy sistemy [Fundamentals of building a subsystem of information security for a multifunctional information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 165-167.
21. *Klepikov E.A., YAs'ko A.O.* Voprosy zashchity konfidentsial'noy meditsinskoy informatsii o patsiente v meditsinskikh informatsionnykh sistemakh [Issues of protecting confidential medical information about a patient in medical information systems], *Simvol nauki* [Symbol of Science], 2016, No. 9-1. Available at: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

Статью рекомендовал к опубликованию д.э.н., профессор Е.Н. Тищенко.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; г. Таганрог, Россия; тел.: +79054530191; д.т.н.; профессор.

Шумилин Александр Сергеевич – e-mail: ashumilin@sfedu.ru; тел.: +79081773495; м.н.с.

Алексеев Дмитрий Михайлович – e-mail: dalekseev@sfedu.ru; тел.: +7951 5069532; ассистент.

Babenko Lyudmila Klimentievna – Southern Federal University; e-mail: lkbabenko@sfedu.ru; Taganrog, Russia; phone: +79054530191; dr. of eng. sc.; professor.

Shumilin Alexander Sergeevich – e-mail: ashumilin@sfedu.ru; phone: +79081773495; junior researcher.

Alekseev Dmitry Mikhailovich – e-mail: dalekseev@sfedu.ru; phone: +79515069532; assistant.

УДК 004.032 DOI 10.18522/2311-3103-2021-5-134-145

С.М. Гушанский, В.Н. Пуховский, В.С. Потапов

РЕАЛИЗАЦИЯ ВЕРОЯТНОСТНОГО ДЕКОДЕРА ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ ДЛЯ КОДОВ СТАБИЛИЗАТОРА

В последнее время наблюдается стремительный рост интереса к квантовым компьютерам. Их работа основана на использовании для вычислений таких квантово-механических явлений, как суперпозиция и запутывание для преобразования входных данных в выходные, которые реально смогут обеспечить эффективную производительность на 3–4 порядка выше, чем любые современные вычислительные устройства, что позволит решать перечисленные выше и другие задачи в натуральном и ускоренном масштабе времени. Данная работа является исследованием влияния среды на квантовую систему кубитов и результаты ее выполнения. Разработан вероятностный декодер глубокой нейронной сети для кодов стабилизатора. Проанализированы и рассмотрены вопросы исправления ошибок для трехбитового кода без декодирования состояния. Актуальность данных исследований заключается в математическом и программном моделировании и реализации корректирующих кодов для исправления нескольких видов квантовых ошибок в рамках разработки и выполнения квантовых алгоритмов для решения классов задач классического характера. Научная новизна данного направления выражается в исключении одного из недостатков квантового вычислительного процесса. Научная новизна данного направления в первую очередь выражается в постоянном обновлении и дополнении поля квантовых исследований по ряду направлений.

Моделирование; квантовый алгоритм; кубит; модель квантового вычислителя; запутывание; суперпозиция; квантовый оператор.

S.M. Gushanskiy, V.N. Pukhovsky, V.S. Potapov

IMPLEMENTATION OF A PROBABLE DEEP NEURAL NETWORK DECODER FOR STABILIZER CODES

Recently, there has been a rapid increase in interest in quantum computers. Their work is based on the use of quantum-mechanical phenomena such as superposition and entanglement for computing to transform input data into outputs that can actually provide effective performance 3–4 orders of magnitude higher than any modern computing devices, which will allow solving the above and other tasks in real and accelerated time scale. This work is a study of the influence of the environment on a quantum system of qubits and the results of its implementation. A probabilistic deep neural network decoder for stabilizer codes has been developed. The issues of error correction for a three-bit code without state decoding are analyzed and considered. The relevance of these studies lies in mathematical and software modeling and implementation of correction codes for correcting several types of quantum errors in the development and implementation of quantum algorithms for solving classes of problems of a classical nature. The scientific novelty of this direction is expressed in the elimination of one of the disadvantages of the quantum computational process. The scientific novelty of this area is primarily expressed in the constant updating and supplementation of the field of quantum research in a number of areas.

Modeling; quantum algorithm; qubit; model of a quantum computer; entanglement; superposition; quantum operator.

Введение. Реализация первого отказоустойчивого логического кубита станет важной вехой в путешествии по созданию квантового компьютера. С этой целью лаборатории в таких местах, как Google, IBM исследователи и TU Delft в настоящее время создают сверхпроводящие устройства с реализациями логического кубита с поверхностным кодом. Кубитовые архитектуры основаны на технологии ионных ловушек и квантовой оптике. Порог для поверхностного кода при реалистичных предположениях относительно шума составляет приблизительно 1 %. Современное оборудование на основе кубитов уже было продемонстрировано с коэффициентом ошибок ниже этого уровня. Однако подавление частоты логических ошибок до такой степени, что логический кубит превосходит некодированный кубит потребует таких уровней масштабируемости, которые пока невозможны в текущих экспериментах. Предполагается, что первые логические кубиты отказоустойчивого поверхностного кода потребуют решетки с более чем тысячей кубитов. Кроме того, достижение этой цели будет только первым шагом: квантовый компьютер только с одним логическим кубитом не будет мощнее, чем счеты с одной бусиной. Фактически, в настоящее время считается, что отказоустойчивый квантовый компьютер с поверхностным кодом, способным превзойти классическое устройство в полезной задаче потребует более миллиона кубитов. Первыми квантовыми протоколами для достижения отказоустойчивости, вероятно, будут коды квантового обнаружения. Как наименьший код, способный защитить от модели квантовой ошибки, код [[4, 2, 2]] является перспективным кандидатом. Несколько экспериментальных реализаций кода [[4, 2, 2]] уже были продемонстрировано в [1–4]. Коды с повторением (из того же семейства, что и двух- и трехкубитные коды) также были реализованы на кубитном оборудовании [5].

За последние пару лет в рамках нескольких проектов аппаратного обеспечения квантовых вычислений были разработаны облачные платформы, чтобы люди могли программировать свои устройства. Мы также должны иметь возможность выполнять операции с закодированными кубитами. Один из способов – декодировать логические кубиты, выполнить с ними операцию и затем перекодировать их. Соответственно, нам нужно уметь делать операции на логических кубитах, пока они кодируются. Дополнительно нам необходимы операции на регулярных этапах исправления ошибок, т.е. измерение синдрома и исправление. Существует 7-кубитный код, который часто используется, потому что он обладает хорошими свойствами: гейт

Адамара на логическом кубите соответствует $H^{\otimes 7}$ на физических кубитах, а CNOT между двумя логическими кубитами соответствует применению CNOT между 7 парами двух блоков физических кубитов (т.е. между 1-м кубитом одного блока и 1-м кубитом другого блока, так далее). Добавление гейт, отображающих $|b\rangle \mapsto e^{ib\pi/4}|b\rangle$ достаточно для универсальных квантовых вычислений. При разработке схем отказоустойчивых вычислений очень важно убедиться, что ошибки не распространяются слишком быстро. Рассмотрим, например, CNOT: если его контрольный бит ошибочен, то после выполнения CNOT также его целевой бит будет ошибочным. Уловка состоит в том, чтобы держать это под контролем таким образом, чтобы регулярные этапы исправления ошибок не были перегружены ошибками. Кроме того, необходимо иметь возможность безотказно готовить состояния и измерять логические кубиты.

1. Каскадные коды и пороговая теорема. Идея объединения кода с самим собой также применима к квантовым кодам. Предположим, у нас есть код (рис. 1), который кодирует один кубит в C кубитов, и допустим, что он может исправить одну ошибку на любом из своих кубитов C, и использует D временных шагов на этап исправления ошибок (каждый временной шаг может включать несколько элементарных вентилей параллельно). Предполагая, что частота ошибок p в один кубит и в один такт работы квантового вычислительного устройства, вероятность отказа кода на конкретном логическом кубите в определенное время равно

$$p' = \sum_{i=2}^{CD} \binom{CD}{i} p^i (1-p)^{CD-i}. \quad (1)$$

Если p – достаточно малая константа, то в этой сумме преобладает член для i = 2, и мы имеем $p' \approx (CD)^2 p^2$. Соответственно, если начальная частота ошибок p ниже некоторой магической постоянной $\approx 1/(CD)^2$, тогда $p' < p$ и, следовательно, каждый уровень исправления ошибок снижает частоту ошибок. В более общем смысле, предположим, что мы объединяем этот код k раз с самим собой. Тогда каждый логический кубит кодируется в кубиты C^k, но частота ошибок для каждого логического кубита уменьшается до $O((CDp)^{2^k})$. Предположим, мы хотим иметь возможность выполнить T = poly(n) тактов без ошибок на логических кубитах. Для этого нужно запустить эффективный квантовый алгоритм на неисправном квантовом оборудовании. Тогда достаточно уменьшить коэффициент ошибок до $<<1/T$, для которого достаточно k=O(loglogT) уровней конкатенации. Эти слои коррекции ошибок увеличивают количество кубитов и время вычислений, но это все еще лишь полилогарифмические накладные расходы. Приведенный выше набросок (при точном его воплощении) дает знаменитую «пороговую теорему» [6, 7]: если начальная частота ошибок квантового оборудования [8] может быть снижена ниже какой-то магической константы (известной как «порог отказоустойчивости»), то можем использовать программные решения, такие как квантовые коды исправления ошибок [9] и отказоустойчивые вычисления, чтобы гарантировать, что можем выполнить квантовые вычисления длительное время без серьезных ошибок. В настоящее время наиболее точные оценки порога составляют около 0,1%, но есть численные доказательства того, что даже несколько процентов могут быть терпимыми. На самом деле это один из самых важных результатов области квантовых вычислений [10], и является основным ответом скептикам: до тех пор, пока экспериментаторам удается реализовать базовые операции в пределах нескольких процентов выявления ошибки масштабируемым образом, тогда мы сможем построить крупномасштабные квантовые компьютеры.

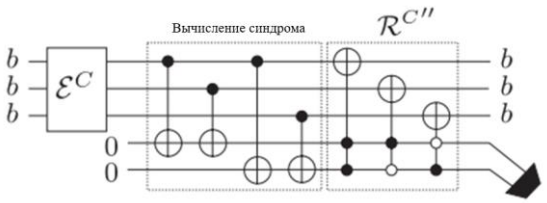

Рис. 1. Исправление ошибок для трехбитового кода без декодирования состояния

Кодовое слово $b_{enc} = bbb$ подвергалось исправляемым ошибкам, что дало строку b_{enc}. В первый этап схемы вычисляется синдром ошибки на вспомогательную, а второй этап схемы [11] исправляет ошибки в b_{enc} на основе синдрома [12]. В общем, если кодируем квантовую информацию [13], подвергаем ее шуму [14] и декодируем (используя обратную операцию кодирования), то не всегда возможно восстановить исходное состояние |ψ>. То есть в некоторых случаях

$$Tr_{anc}[U'_{enc}(\sum \varepsilon_i^Q |\psi_{enc}\rangle\langle\psi_{enc}|\varepsilon_i^{Q'})U_{enc}] \neq |\psi\rangle\langle\psi|. \quad (2)$$

Для восстановления квантовой информации нам понадобится квантовая операция R^Q, называемая операцией восстановления [15], которая имеет эффект устранения достаточного количества шума на закодированное состояние, так что после декодирования и отслеживания анцилла [16] кубита у нас остается исходное состояние |ψ>, как показано на рис. 2.

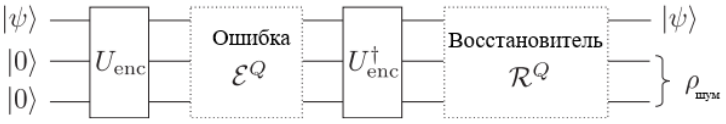

Рис. 2. Восстановление квантовой информации

В общем случае операция восстановления R^Q будет супероператором, определенным в терминах суммы по некоторым операторам R_j^Q. Для данного кода, подверженного шуму, описанному E_i^Q, определяем точность операции восстановления R на

$$F(R,C,E) = \min_{|\psi\rangle} \langle\psi|p_\psi|\psi\rangle, \quad (3)$$

где

$$p_\psi = Tr_{anc}(\sum_j R_j^Q U'_e(\sum_i E_i^Q U_{enc}|\psi\rangle|00...0\rangle\langle 00...0|\langle\psi|U'_{enc}E_i^{Q'})U_e R_j^{Q'}) \quad (4)$$

и соответствующий параметр вероятности ошибки наихудшего случая p равен p = 1 – F(R, C, E). Стоит пояснить значение приведенного выше определения. Предположим какое-то состояние |ψ> кодируется в состояние U|ψ>|00. . .0>, затем подвергается некоторому шуму, затем подвергается операции восстановления (соответствует операторам R_j^Q), а затем вспомогательное рабочее пространство отбрасывается, возвращая некоторое состояние p_ψ в исходном гильбертовом пространстве. Мы заинтересованы в получении насколько возможно близкому значению ρ к исходному состоянию |ψ><ψ|. Вероятность $p_\psi = \langle\psi|p_\psi|\psi\rangle$ следует рассматривать как вероятность от-

сутствия ошибки в закодированном состоянии. Количество F(R, C, E) – это минимум всех таких вероятностей p_ψ по всем кодированным состояниям |ψ>. Таким образом, параметр вероятности ошибки дает нам верхнюю границу вероятности, с которой общее закодированное состояние закончится в неправильном состоянии (строго говоря, его квадратный корень – это амплитуда вероятности [17], с которой произошла ошибка). Операция восстановления (рис. 3) R^Q является исправлением ошибок по отношению к набору операторов ошибок, если параметр вероятности ошибки p равен нулю, когда R^Q применяется к кодовому слову, которое было показано только этим операторам ошибок. Это означает, что

$$Tr_{anc}[\sum_j R_j^Q(U_{enc}^{'}(\sum E_i^Q|\psi_{enc}\rangle\langle\psi_{enc}|E_i^{Q'})U_{enc})R_j^{Q'}] = |\psi\rangle\langle\psi|. \quad (5)$$

Один из способов думать о действии операции восстановления R^Q состоит в том, что она выталкивает весь шум во вспомогательную, так что ошибки устраняются. Операцию кодирования можно рассматривать как способ преобразование ошибок таким образом, чтобы их действие на закодированные состояния можно было исправить. Подставляя $|\psi_{enc}\rangle = U_{enc}|\psi\rangle|00...0\rangle$ в выражение в левой части уравнения выше, имеем

$$\sum_j R_j^Q(U_{enc}^{'}(\sum_i E_i^Q U_{enc}|\psi\rangle|00...0\rangle\langle 00...0|\langle\psi|U^{'}{}_{enc}E_i^{Q'})U_{enc})R_j^{Q'}. \quad (6)$$

Можем думать об операторах $U^{'}{}_{enc}E_i^{Q'}U_{enc}$ как о преобразованных ошибках, действующий на |ψ>|00…0>. Цель состоит в том, чтобы выбрать U_{enc} таким образом, чтобы поведение преобразованных ошибок позволяет нам найти операцию восстановления R^Q, которая дает нам $|\psi\rangle\langle\psi| \otimes p_{noise}$ (шум в целом будет смешанным состоянием, поэтому мы записали конечное состояние с матрицей плотности [18]). Для кода с двумя логическими кодовыми словами, применяя U_{enc} к вычислительной базе состояния |0> и |1> создают кодовые слова $|0_{enc}\rangle$ и $|1_{enc}\rangle$ соответственно. Чтобы код был полезным, должна существовать операция восстановления R^Q, удовлетворяющая уравнению 5 как для $|0_{enc}\rangle$ так и для $|1_{enc}\rangle$. Можно показать (длительным расчетом), что для существования такого R^Q мы должны иметь

$$\langle l_{enc}|E_i^{Q'}E_i^Q|m_{enc}\rangle = c_{ij}\partial_{lm} \quad (7)$$

для l, m ∈ {0,1}, где c_{ij} – константы. Уравнение 6 дает условия для квантовой коррекции ошибок.

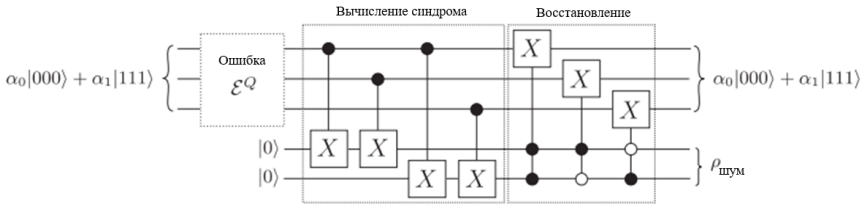

Рис. 3. Операция восстановления трехкубитового флип-кода [19] путем вычисления синдрома ошибки, а затем управление операцией восстановления

2. Реализация вероятностного декодера глубокой нейронной сети для кодов стабилизатора. Нейронные сети [20] являются особенно эффективными инструментами для аппроксимации [21] функций, где функция f: x → f(x) должна быть изучена из большого количества обучающих данных, представленных в виде пар (x, f(x)). Вход x устанавливается как значение входного слоя [22] нейронов. Каждый из этих нейронов через аксоны [23] связан с каждым нейроном следующего слоя. Таким образом, можно соединить вместе несколько скрытых слоев нейронов, чтобы построить более глубокую [24] нейронную сеть. Последний уровень сети – это выходной слой – его значение представляет собой изученное f(x). Значение нейрона (то есть значение его активации) рассчитывается как взвешенная сумма значений активации нейронов, подключенных к нему из предыдущего слоя. Затем эта сумма передается через нелинейную функцию (называемую функцией активации). Это значение активации затем передается нейронам следующего слоя, где процесс повторяется, пока не достигнет выходного слоя. Веса в суммах (т.е. сила связей между нейронами) – это параметры, которые оптимизируются с помощью стохастического градиентного спуска, чтобы минимизировать расстояние между изученным f и f, вычисленным на основе данных обучения. Выбор функции активации, размер скрытых слоев и размер шага для градиентного спуска [25] (также называемые гиперпараметрами) решаются заранее, до обучения. Текущие передовые практики включают выполнение случайного поиска для поиска лучших гиперпараметров.

В частном случае декодирования кода коррекции квантовой ошибки стабилизатора [26] мы хотим сопоставить синдромы с соответствующими физическими ошибками, следовательно, мы принимаем входной уровень как синдром (полученный при измерении стабилизаторов). Например, для торического кода (рис. 4) с размером решетки 9 на 9 мы должны измерить 162 входных нейронов (имеющего значение 0, если синдром тривиальный, и 1, если нет). Точно так же устанавливаем выходной уровень для предсказания того, какие физические ошибки произошли (обычно они представлены на картинке Гейзенберга, благодаря теореме Готтесмана-Книлла). Используя тот же пример, у нас есть 162 физических кубита, и нужно отслеживать их собственные значения с помощью операторов Z и X, что требует в общей сложности 324 выходных нейронов (со значением 0, если ошибок не было, и значением 1 в противном случае). Чтобы полностью определить архитектуру нейронной сети, устанавливаем для функций активации скрытых слоев значение тангенса, а для активации выходного слоя – сигмовидную функцию $\sigma(x) = (1 - e^{-x})^{-1} \in [0,1]$. Размер скрытого слоя был установлен в четыре раза больше размера входного слоя. Эти решения были приняты после исчерпывающего перебора возможных гиперпараметров, проверенных на торических кодах расстояния от 3 до 6, и оказалось, что они хорошо работают и для более крупных кодов.

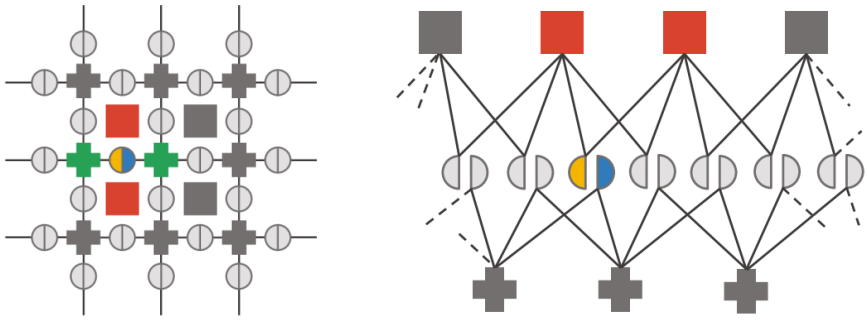

Рис. 4. Торический код квантовой коррекции ошибок

Количество скрытых слоев варьировалось более глубокие сети дают лучшее приближение вплоть до точки уменьшения отдачи около 15 слоев. Размер шага для градиентного спуска (он же скорость обучения) был отожжен – постепенно уменьшен, чтобы позволить быстро достичь минимума. Мера расстояния между данными обучения и оценки, которая сводится к минимуму с помощью градиентного спуска – это их бинарная кроссэнтропия (мера разницы между двумя распределениями вероятностей). Обучение проводилось более одного миллиарда (синдром, ошибка) пар партиями по 512, что потребовало около суток рабочего времени графического процессора для торического кода 5 на 5. Пары генерировались на лету, сначала генерируя ошибку выборки из данной модели ошибок (этот обучающий набор также можно эффективно сгенерировать непосредственно на экспериментальном оборудовании), а затем получая соответствующий синдром с помощью скалярного произведения с матрицей проверки на четность.

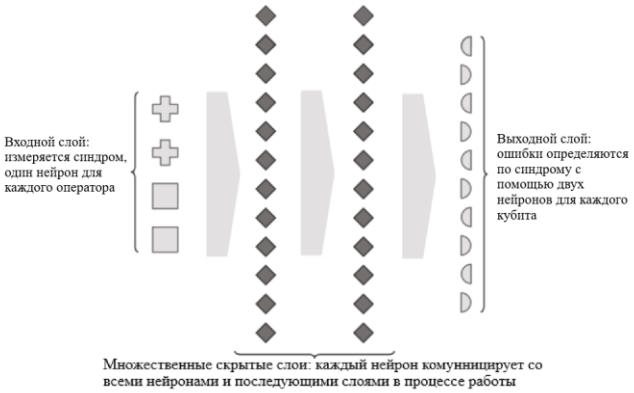

Рис. 5. Декодер нейронной сети

Модель ошибки, используемая для каждого физического кубита, представляла собой деполяризацию кубита, параметризованную точностью кубита p – вероятностью отсутствия ошибки на данном кубите или, что эквивалентно, скоростью деполяризации 1 – p. Согласно этой модели, ошибки Z, X и Y (последовательные Z и X) имели равные вероятности 1/3(1 – p). Для каждого значения p обучили новую сеть, однако результаты показали некоторую устойчивость к тестированию нейронной сети с частотой ошибок, отличной от той, на которой она была обучена. Производительность сети будет улучшена, если нормализовать входные значения, чтобы получить среднее значение 0 и стандартное отклонение 1. Для коэффициента ошибок деполяризации 1 – p скорость, с которой изменяется собственное значение Z, составляет $p_e = \frac{2}{3}(1-p)$. В примере торического кода скорость нетривиальных измерений стабилизатора будет одинаковой для Z и для X, а именно $p_s = 4q^3(1-q) + 4q(1-q)^3$, а дисперсия будет $v_s = p_s - p_s^2$. Обученная сеть может эффективно оценивать приближение функции декодирования, поэтому все, что Алисе нужно сделать, чтобы выполнить для исправления ошибок в ее квантовой памяти заключается в измерении синдрома и запуске нейронной сети для оценки синдрома. Однако нейронная сеть является непрерывной функцией и несовершенным приближением, поэтому значения в синдроме не будут дискретными нулями и единицами, а будут действительными числами от нуля до единицы. Распространенный способ использования и интерпретации этих значений – рассматривать их

как распределение вероятностей возможных ошибок, т.е. i-е значение в массиве синдрома – это действительное число от нуля до единицы, равное вероятности i-го кубита перевернуться (половина массива соответствует Z ошибкам, а половина массива соответствует X ошибкам). Эта интерпретация подкрепляется использованием бинарной кроссэнтропии в качестве цели оптимизации во время обучения. Чтобы определить, какая ошибка произошла, выбираем это распределение вероятностей. Далее проверяем правильность выборки, вычисляя синдром, который может вызвать предсказанная ошибка – если он отличается от данного синдрома, повторяем выборку. Передискретизируем только кубиты, участвующие в измерении стабилизатора, соответствующие неверным элементам синдрома (рис. 6).

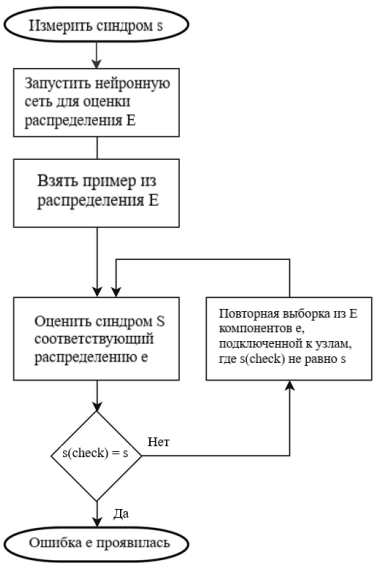

Рис. 6. Выборка нейронной сети

На первый взгляд реализация декодера (рис. 5) может выглядеть как реализация таблицы поиска, однако подчеркнем огромное сжатие данных, которого достигает нейронная сеть. Во-первых, можно рассмотреть размер самой нейронной сети. Для кода на N физических кубитов количество параметров, необходимых для описания нейронного декодера L уровней, будет $O(N^2L)$. Более того, размер обучающего набора данных для тестируемых нами кодов не превышал 10 миллиардов, и его можно уменьшить на несколько порядков, если повторно использовать образцы в стохастическом градиентном спуске (общий подход, используемый при обучении). С другой стороны, размер полной таблицы поиска будет порядка $O(4^N)$. Даже если возьмем только наиболее вероятные ошибки (и отбросим ошибки с вероятностью менее 5%), при скорости деполяризации 0,1 понадобится таблица поиска больше 1012 для торического кода с расстоянием 5 (50 кубитов), больше чем 1023 для торического кода расстояния 7 (98 кубитов) и больше 1037 для торического кода расстояния 9 (162 кубита).

Благодаря этому сжатию, прямой оптимизации для наиболее вероятной ошибки и простоте включения информации о корреляциях ошибок в процедуру декодирования, представленный здесь алгоритм является одним из лучших вариантов для декодирования кодов стабилизатора менее 200 кубитов. Из-за вероятно-

стного характера выборки декодер становится практически неэффективным для кодов размером более примерно 200 кубитов. Это можно отнести к двум характеристикам алгоритма: используем простую передачу сообщений с жестким решением, алгоритм в выборке вместо более продвинутого алгоритма распространения убеждений, засеянного выходными данными нейронной сети. Кроме того, нейронная сеть изучает только предельные вероятности ошибок на каждом кубите, не обеспечивая корреляции между этими ошибками. Более продвинутая нейронная сеть могла бы решить эту проблему, предоставив корреляционную информацию на своем выходном уровне.

На рис. 7 пунктирными линиями показаны характеристики декодера для тех же кодов, что и для эталона. Коды на расстоянии до 9 (содержащие 162 физических кубитов) практичны, но расширение использования декодера для кодов с более чем 242 физическими кубитами было бы недопустимо из-за накладных расходов на выборку. Оценки проводились для скорости деполяризации 10% физических кубитов.

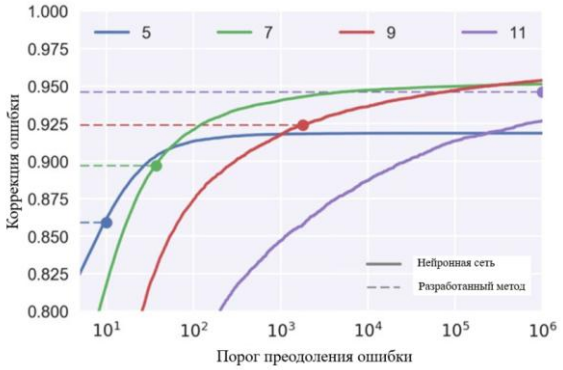

Рис. 7. Накладные расходы на выборку в зависимости от производительности декодера. На графике представлена производительность декодера, обученного на торических кодах разных расстояний по максимально допустимому количеству итераций

Хотя этот декодер является общим и может применяться к любому коду стабилизатора, можно также разработать архитектуру нейронных сетей, которые специально используют решетчатую структуру и трансляционную симметрию торического кода. Например, сверточные нейронные сети хорошо адаптированы для обработки 2D-данных. Более того, благодаря трансляционной симметрии можно представить себе декодер, который обучается на фиксированном фрагменте кода, и его можно использовать для торических кодов любого размера.

Заключение. В настоящее время активно развивается теория квантовых вычислений. Несмотря на то, что идея квантового компьютера была высказана еще Р. Фейнманом в 1982 г. До сих пор проводятся научные исследования по этой тематике. Исправление ошибок – одна из основных задач, стоящих перед квантовыми вычислительными устройствами. И без решения данной проблемы, дальнейшие успешные разработки в этой многообещающей области станут неэффективными. В данной работе численно смоделированы коды коррекции различных видов ошибок. Проанализированы основные препятствия и трудности на пути защиты канала от шума, а также предложены некоторые методы их преодоления. Произведена реализация схем исправления основных типов квантовых ошибок.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-07-00916.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Calderbank A.R., Shor P.W.* Good quantum error-correcting codes exist // Phys Rev A. – 1996. – Vol. 54. – P. 1098-1106.
2. *Linke N.M., Gutierrez M., Landsman K.A., et al.* Fault-tolerant quantum error detection // Science Advances. – 2017. – 3 (10): e1701074. Available from: https://doi.org/10.1126/sciadv.1701074.
3. *Vuillot C.* Is error detection helpful on IBM 5q chips? // Quantum Information and Computation. – 2018. – Vol. 18, No. 11-12. – P. 0949-0964.
4. *Harper R., Flammia S.T.* Fault-tolerant logical gates in the IBM quantum experience // Phys Rev Lett. – 2019. – 122:080504. Available from: https://link.aps.org/doi/10.1103/PhysRevLett. 122.080504.
5. *Wootton J.R., Loss D.* Repetition code of 15 qubits // Physical Review A. – 2018. – Vol. 97 (5). Available from: https://doi.org/10.1103/physreva.97.052313.
6. *Aspuru-Guzik A., Dutoi A.D., Love P.J., et al.* Simulated quantum computation of molecular energies // Science. – 2005. – Vol. 309 (5741). – P. 1704-1707. Available from: https://science.sciencemag.org/content/309/5741/1704.
7. *Knill M., Laflamme R., and Zurek W.* Threshold accuracy for quantum computation. – quantph/9610011, 15 Oct 1996.
8. *Гушанский С.М., Потапов В.С.* Методика разработки и построения квантовых алгоритмов // Информатизация и связь. – 2017. – № 3. – С. 101-104.
9. *Гушанский С.М., Поленов М.Ю., Потапов В.С.* Реализация компьютерного моделирования системы с частицей в одномерном и двухмерном пространстве на квантовом уровне // Известия ЮФУ. Технические науки. – 2017. – № 6 (191). – С. 223-233.
10. *Гузик В.Ф., Гушанский С.М., Потапов В.С.* Количественные характеристики степени запутанности // Известия ЮФУ. Технические науки. – 2016. – № 3 (176). – С. 76-86.
11. *Kleppner D., Kolenkow R.* An Introduction to Mechanics (Second ed.). – Cambridge: Cambridge University Press, 2014. – 49 p.
12. *Потапов В.С., Гушанский С.М.* Квантовые типы ошибок и методы их устранения, зависимость ошибки от меры и чистоты запутанности // Сб. трудов XIV Всероссийской научной конференции молодых ученых, аспирантов и студентов ИТСАиУ-2016. – Ростов-на-Дону: Изд-во ЮФУ, 2016. – Т. 3. – С. 123-129.
13. *Gushansky S., Pykhovskiy V., Kozlovskiy A., Potapov V.* Development of a scheme of a hardware accelerator of quantum computing for correction quantum types of errors // The 4-th Computational Methods in Systems and Software 2020, Czech Republic. – P. 64-73.
14. *Hales S.* Hallgren An improved quantum Fourier transform algorithm and applications // Proceedings of the 41st Annual Symposium on Foundations of Computer Science. November 12–14, 2000. – P. 515.
15. *Guzik V., Gushanskiy S., Polenov M., Potapov V.* Complexity Estimation of Quantum Algorithms Using Entanglement Properties // 16th International Multidisciplinary Scientific GeoConference, Bulgaria, 2016. – P. 20-26;
16. *Guzik V., Gushanskiy S., Polenov M., Potapov V.* Models of a quantum computer, their characteristics and analysis // 9th International Conference on Application of Information and Communication Technologies (AICT). – Institute of Electrical and Electronics Engineers, 2015. – P. 583-587.
17. *Collier D.* The Comparative Method. In: Finifter A.W. (ed.) Political Sciences: The State of the Discipline II. pp. 105-119: American Science Association. – Washington, DC, 1993.
18. *Olukotun K.* Chip Multiprocessor Architecture – Techniques to Improve Throughput and Latency. Morgan and Claypool Publishers, San Rafael, 2007.
19. *Raedt K.D., Michielsen K., De Raedt H., Trieu B., Arnold G., Marcus Richter, Th Lip-pert, Watanabe H., and Ito N.* Massively parallel quantum computer simulator // Computer Physics Communications. – 2007. – Vol. 176. – P. 121-136.
20. *Williams C.P.* Explorations in Quantum Computing. Texts in Computer Science, Chapter 2. Quantum Gates, Springer, 2011. – P. 51-122.
21. *Potapov V., Gushanskiy S., Guzik V., Polenov M.* The Computational Structure of the Quantum Computer Simulator and Its Performance Evaluation // In: Software Engineering Perspectives and Application in Intelligent Systems. Advances in Intelligent Systems and Computing. – Springer, 2019. – Vol. 763. – P. 198-207.

22. *Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V.* Entanglement-assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem // IEEE Transactions on Information Theory. – 2002. – Vol. 48. – P. 2637-2655.
23. *Milner R.G.* A Short History of Spin. In: Contribution to the XV International Workshop on Polarized Sources, Targets, and Polarimetry. – Charlottesville, Virginia, USA, September 9–13, 2013. – arXiv:1311.5016 (2013).
24. *Hallgren H.S.* An improved quantum Fourier transform algorithm and applications // In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA. IEEE, 2000. – P. 515.
25. *Boneh D., Zhandry M.* Quantum-secure message authentication codes // In: Proceedings of Eurocrypt. – 2013. – P. 592-608.
26. *Potapov V., Gushansky S., Guzik V., Polenov M.* Architecture and Software Implementation of a Quantum Computer Model // In: Advances in Intelligent Systems and Computing. – Springer, 2016. – Vol. 465. – P. 59-68.

REFERENCES

1. *Calderbank A.R., Shor P.W.* Good quantum error-correcting codes exist, *Phys Rev A*, 1996, Vol. 54, pp. 1098-1106.
2. *Linke N.M., Gutierrez M., Landsman K.A., et al.* Fault-tolerant quantum error detection, *Science Advances*, 2017, 3 (10): e1701074. Available from: https://doi.org/10.1126/sciadv.1701074.
3. *Vuillot C.* Is error detection helpful on IBM 5q chips?, *Quantum Information and Computation*, 2018, Vol. 18, No. 11-12, pp. 0949-0964.
4. *Harper R., Flammia S.T.* Fault-tolerant logical gates in the IBM quantum experience, *Phys Rev Lett.*, 2019. 122:080504. Available from: https://link.aps.org/doi/10.1103/PhysRevLett.122.080504.
5. *Wootton J.R., Loss D.* Repetition code of 15 qubits, *Physical Review A*, 2018, Vol. 97 (5). Available from: https://doi.org/10.1103/physreva.97.052313.
6. *Aspuru-Guzik A., Dutoi A.D., Love P.J., et al.* Simulated quantum computation of molecular energies, *Science*, 2005, Vol. 309 (5741), pp. 1704-1707. Available from: https://science.sciencemag.org/content/309/5741/1704.
7. *Knill M., Laflamme R., and Zurek W.* Threshold accuracy for quantum computation. quantph/9610011, 15 Oct 1996.
8. *Gushanskiy S.M., Potapov V.S.* Metodika razrabotki i postroeniya kvantovykh algoritmov [Methodology of development and construction of quantum algorithms], *Informatizatsiya i svyaz'* [Informatization and communication], 2017, No. 3, pp. 101-104.
9. *Gushanskiy S.M., Polenov M.Yu., Potapov V.S.* Realizatsiya komp'yuternogo modelirovaniya sistemy s chastitsey v odnomernom i dvukhmernom prostranstve na kvantovom urovne [Implementation of computer simulation of a system with a particle in one-dimensional and two-dimensional space at the quantum level], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 6 (191), pp. 223-233.
10. *Guzik V.F., Gushanskiy S.M., Potapov V.S.* Kolichestvennye kharakteristiki stepeni zaputannosti [Quantitative characteristics of the degree of entanglement], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 3 (176), pp. 76-86.
11. *Kleppner D., Kolenkow R.* An Introduction to Mechanics (Second ed.). Cambridge: Cambridge University Press, 2014, 49 p.
12. *Potapov V.S., Gushanskiy S.M.* Kvantovye tipy oshibok i metody ikh ustraneniya, zavisimost' oshibki ot mery i chistoty zaputannosti [Quantum types of errors and methods of their elimination, the dependence of error on the measure and purity of entanglement], *Sb. trudov XIV Vserossiyskoy nauchnoy konferentsii molodykh uchenykh, aspirantov i studentov ITSAiU-2016* [Proceedings of the XIV All-Russian Scientific Conference of Young Scientists, postgraduates and students of ITSAiU-2016]. Rostov-on-Don: Izd-vo YuFU, 2016, Vol. 3, pp. 123-129.
13. *Gushansky S., Pykhovskiy V., Kozlovskiy A., Potapov V.* Development of a scheme of a hardware accelerator of quantum computing for correction quantum types of errors, *The 4-th Computational Methods in Systems and Software 2020, Czech Republic*, pp. 64-73.
14. *Hales S.* Hallgren An improved quantum Fourier transform algorithm and applications, *Proceedings of the 41st Annual Symposium on Foundations of Computer Science. November 12–14, 2000*, pp. 515.

15. *Guzik V., Gushanskiy S., Polenov M., Potapov V.* Complexity Estimation of Quantum Algorithms Using Entanglement Properties, *16th International Multidisciplinary Scientific GeoConference, Bulgaria, 2016*, pp. 20-26;
16. *Guzik V., Gushanskiy S., Polenov M., Potapov V.* Models of a quantum computer, their characteristics and analysis, *9th International Conference on Application of Information and Communication Technologies (AICT)*. Institute of Electrical and Electronics Engineers, 2015, pp. 583-587.
17. *Collier D.* The Comparative Method. In: Finifter A.W. (ed.) Political Sciences: The State of the Discipline II. pp. 105-119: American Science Association. Washington, DC, 1993.
18. *Olukotun K.* Chip Multiprocessor Architecture – Techniques to Improve Throughput and Latency. Morgan and Claypool Publishers, San Rafael, 2007.
19. *Raedt K.D., Michielsen K., De Raedt H., Trieu B., Arnold G., Marcus Richter, Th Lip-pert, Watanabe H., and Ito N.* Massively parallel quantum computer simulator, *Computer Physics Communications*, 2007, Vol. 176, pp. 121-136.
20. *Williams C.P.* Explorations in Quantum Computing. Texts in Computer Science, Chapter 2. Quantum Gates, Springer, 2011, pp. 51-122.
21. *Potapov V., Gushanskiy S., Guzik V., Polenov M.* The Computational Structure of the Quantum Computer Simulator and Its Performance Evaluation, *In: Software Engineering Perspectives and Application in Intelligent Systems. Advances in Intelligent Systems and Computing*. Springer, 2019, Vol. 763, pp. 198-207.
22. *Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V.* Entanglement-assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem, *IEEE Transactions on Information Theory*, 2002, Vol. 48, pp. 2637-2655.
23. *Milner R.G.* A Short History of Spin. In: Contribution to the XV International Workshop on Polarized Sources, Targets, and Polarimetry. Charlottesville, Virginia, USA, September 9–13, 2013. arXiv:1311.5016 (2013).
24. *Hallgren H.S.* An improved quantum Fourier transform algorithm and applications, *In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA. IEEE, 2000*, pp. 515.
25. *Boneh D., Zhandry M.* Quantum-secure message authentication codes, *In: Proceedings of Eurocrypt*, 2013, pp. 592-608.
26. *Potapov V., Gushansky S., Guzik V., Polenov M.* Architecture and Software Implementation of a Quantum Computer Model // In: Advances in Intelligent Systems and Computing. Springer, 2016, Vol. 465, pp. 59-68.

Статью рекомендовал к опубликованию д.т.н., профессор В.И. Божич.

Гушанский Сергей Михайлович – Южный федеральный университет, e-mail: smgushanskiy@sfedu.ru; г. Таганрог, Россия; тел.: 88634371656; кафедра вычислительной техники; к.т.н.; доцент.

Пуховский Валерий Николаевич – e-mail: vpuhovskiy@sfedu.ru; кафедра вычислительной техники; к.т.н.; доцент.

Потапов Виктор Сергеевич – e-mail: vitya-potapov@rambler.ru; кафедра вычислительной техники; ассистент.

Gushanskiy Sergey Mikhailovich – Southern Federal University; e-mail: smgushanskiy@sfedu.ru; Taganrog, Russia; phone: +78634371656; the department of computer engineering; cand. of eng. sc.; associate professor.

Pukhovsky Valery Nikolaevich – e-mail: vpuhovskiy@sfedu.ru; the department of computer engineering; cand. of eng. sc.; associate professor.

Potapov Viktor Sergeevich – e-mail: vitya-potapov@rambler.ru; the department of computer engineering; assistant.